Evaluated Configuration for Oracle Internet Directory 10*g* (10.1.4.0.1)

March 2008

Security Evaluations
Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065

Evaluated Configuration for Oracle Internet Directory 10*g* (10.1.4.0.1)

March 2008

Author: Peter Goatly.

Contributors: James Belton, Julian Skinner, Adam O'Brien.

Contents

Contents

CHAPTER

1 Introduction

The Target of Evaluation (TOE) is Oracle Internet Directory 10*g* (10.1.4.0.1).

The TOE is hosted on the Red Hat Enterprise Linux AS Version 4 Update 5 operating system platform and uses the Oracle Database 10*g* Release 2 (10.1.0.5.0) Object-Relational Database Management System to hold its directory data.

This document explains the manner in which the TOE must be configured along with the host operating system, Oracle database, and network services so as to provide the security functionality and assurance as required under the Common Criteria for Information Technology Security Evaluation [CC].

The assumptions and procedures stated in the document are intended to remove potential vulnerabilities or attack paths from the TOE in its environment. They do not have any impact on the correct implementation of the TOE's SFs.

The Evaluation Assurance Level for the TOE is EAL4 augmented with ALC_FLR.3. The Security Target used for the evaluation of the TOE is [ST].

1.1 Intended Audience

The intended audience for this document includes evaluators of the TOE, system integrators who will be integrating the TOE into systems, and accreditors of the systems into which the TOE has been integrated.

1.2 Organization

This document is composed of the following chapters:

Chapter 1 contains the introduction to the document;

Chapter 2 describes the preparatory actions to be undertaken before installing the software for the evaluated configuration;

Chapter 3 describes the installation of the software for the evaluated configuration;

Chapter 4	describes the post-installation actions to complete the evaluated configuration;
Chapter 5	describes the supporting procedures to ensure that the TOE is operated in a way that upholds the security objectives defined in [ST];
Annex A	lists the TOE components installed as per Chapter 3;
Annex B	describes the steps required to install the operating system underlying the TOE; and
Annex C	lists the references that are used in this document.

Change bars indicate changes since the previous issue.

1.3 Format

Assertions about the configuration actions that are required to be performed are given identifiers to their left in bold Helvetica font, e.g. **[A-1]**. References to sections of documents listed in Annex B are in the format [*document, section*].

The identifiers for assertions are left unchanged from those used for the same assertions in [ECD904].

Mandatory evaluation configuration requirements use the words “must” and/or “shall” in each assertion.

Strongly recommended evaluation configuration requirements use the words “should” in each assertion.

CHAPTER

2 Preparation

This chapter describes the preparatory actions to be undertaken before installing the software for the evaluated configuration.

2.1 Machine Configuration

In the Evaluated Configuration for Oracle Internet Directory 10*g* (10.1.4.0.1) the machine allocated for the installation of the TOE is specified in the table below.

Machine	SagDell3t
Specification	Dell PowerEdge1950 2x Intel Xeon Dual Core Processors 16GB Memory RedHat Enterprise Linux AS Release 4 Update 5
Products to be installed	Oracle Internet Directory 10.1.4.0.1 Oracle Database 10.1.0.5.0

Table 2-1: Server Machine Running the TOE

2.2 Physical Environmental Assumptions

The physical requirements on the server machine so that it can be used for running the TOE while maintaining the security of the database system underlying the TOE are given in [DBECD, 2.1]. This section describes physical requirements on the server machine so that the security of the TOE can be maintained.

[DI.A-1] The processing resources of the TOE shall be located within controlled access facilities which will prevent unauthorized physical access to the TOE by unprivileged us-

ers. Only authorised administrators for the system hosting the TOE shall have physical access to that system. Such administrators include the Operating System Administrators, Database Administrators and OID Directory Administrators.

[DI.A-2] The media on which the TOE audit data resides shall not be physically removable from the underlying operating system by unauthorised users.

[DI.A-3] Any on-line and/or off-line storage media on which security relevant data resides shall be located within controlled access facilities which will prevent unauthorised physical access.

2.3 Electronic Delivery of the TOE

To receive electronic delivery of the TOE installation software, complete the following steps:

1. Access the Oracle's Technet Website at http://technet.oracle.com.
2. Click on the 'Downloads' link.
3. Scroll down to the Middleware section and click 'Identity Management'.
4. Click the checkbox if you agree to the Licence Terms and export restrictions.
5. Click the 'I Accept' button to agree to the OTN licence terms.
6. You should now be looking at the 'Oracle Identity Management 10*g* 10.1.4.0.1 Downloads' page: http://www.oracle.com/technology/software/products/ias/htdocs/10401.htm.
7. The following product needs to be downloaded for the Linux operating system:

   - Oracle Identity Management Infrastructure and Oracle Federation

8. Hovering the mouse pointer over the link to the download will display the download's cksum number. This number should be recorded for later verification.

9. When the first download is requested, the OTN Sign-in page is presented.

10. Complete the form with your OTN login details, or create an account by clicking 'sign up now'.

11.The download will start. Again, ensure that you download each disk.

12. Once the download is complete and the file has been transferred to the target environment, check the file with the cksum filename command to ensure that the download has not become corrupted. If the CKSUM numbers do not match, the file should be downloaded again.

For the Evaluated Configuration, the RedHat operating system software was obtained via download from the RedHat Network web site and made available to the host servers via an NFS mount.

2.4 Physical Delivery of the TOE

To request the media pack:

Go to www.oracle.com and select Shop Online. Choose the appropriate store and select Application Server. Select Application Server Enterprise Edition and chose your licensing terms. Select 'Purchase Media Packs'. Select Linux x86. Then select Oracle® Application Server 10g Release 2 (10.1.2.0.2) Media Pack (with Oracle® Enter-

prise Manager 10g Release 3 Grid Control (10.2.0.3.0)) for Linux x86 (32-bit).

When the media pack arrives the relevant CDs / DVDs are:

B30971-01 – Oracle Identity Management Infrastructure and Oracle Identity Federation (10.1.4.0.1) (CD 1 of 2)

B30972-01 – Oracle Identity Management Infrastructure and Oracle Identity Federation (10.1.4.0.1) (CD 2of 2)

This Page Intentionally Blank

CHAPTER

3 Installation

This chapter describes the installation of the software for the evaluated configuration.

3.1 Operating System Installation / Configuration

The actions **[DI.PRE-1]** to **[DI.PRE-6]** listed in this section are required before the installation of the TOE can be carried out.

[DI.PRE-1] Red Hat Enterprise Linux AS Version 4 Update 5 shall be installed as described in Annex B.

[DI.PRE-2] In order that the Oracle Application Server 10*g* (10.1.4.0.1) installation process can install the TOE successfully, the following lines must be present in the file `/etc/sysctl.conf`:

```
kernel.shmall = 2097152
kernel.shmmax = 2147483648
kernel.shmmni = 4096
kernel.sem = 256 32000 100 142
fs.file-max = 131072
net.ipv4.ip_local_port_range = 1024 65000
kernel.msgmni = 2878
kernel.msgmax = 8192
kernel.msgmnb = 65535
```

[DI.PRE-3] An operating system group, which will be used by the Oracle software owner and database administrators, must be created before installing the TOE. Any legal name can be used for this group, but the convention is to use “oinstall”. The oinstall group can be created via the admintool GUI or with the Linux command:

```
$ groupadd oinstall
```

[DI.PRE-3] An operating system user that will be the Oracle software owner must be created before installing the TOE. The standard name used is “oracle”. When creating the user a primary group is required. The primary group should be oinstall. The oracle user can

be created via the admintool GUI or with the Linux command:

```
$ useradd -g oinstall -c "Oracle Software Owner" oracle
$ passwd oracle
```

[DI.PRE-4] The server machine should have a directory within which the TOE installation media will be stored. In the Evaluated Configuration this was: `/space/src/oracle`.

Also, the server should have a directory into which the software will be installed. In the Evaluated Configuration this was: `/space/oracle/product`

The following commands can be used to configure the ownership and access rights for these directories:

```
chown -R oracle:oinstall /space/src
chown -R oracle:oinstall /space/oracle
chmod 755 /space/src/oracle
chmod 755 /space/oracle/product
```

[DI.PRE-5] Configure the firewall on the server machine as follows:

From the desktop as `root` select:

```
Applications
System Settings
Security Level
```

From the Security Level Configuration application select the following:

Security Level: Enable Firewall
Other ports: 389: tcp

Click OK

Click Yes

Restart the firewall with the following command:

```
$ /sbin/service iptables restart
```

[DI.PRE-6] Create the directory `OIM_ID_INFRA` within the directory `/space/src/oracle/OIM_ID_INFRA` to hold the OID issue media.

If the installation files for Oracle Internet Directory 10*g* (10.1.4.0.1) were obtained via CD or DVD then the contents of the CDs or DVDs should be copied into the corresponding directory and uncompressed if required. If the installation files were obtained via download, the downloaded file should be copied into the corresponding directory and uncompressed using the following syntax:

```
$ cpio -idm < file_name.cpio
```

3.2 Oracle Internet Directory Installation

3.2.1 Installation of Oracle Internet Directory 10*g* (10.1.4.0.1)

[OIDIG] describes the steps needed to install the TOE and the Oracle Database it uses.

Any prior installations of Oracle Application Server must have been removed before this installation process starts. [INST] may be read for general guidance when install-

ing the TOE software.

3.2.2 Exclusions

Section A.1 covers the process by which software components are installed on the server by the Oracle Universal Installer during the installation of Oracle Internet Directory 10*g* (10.1.4.0.1) as per the section above. Because this is an Application Server installation process, many of these components are not part of the TOE. Section A.2 lists the components that actually constitute the TOE. The other components are only to be used if they are essential for the use of the TOE in its evaluated configuration.

3.3 Client Installation

The TOE scope does not include any client software. During the evaluation of the TOE, software on a client machine can be used to send LDAP messages to the TOE in order to test its security features. Administrators are to prevent other client software being installed on any machine in the network that includes the evaluated configuration of the TOE as per the following assertion:

[DI.CA-1] No applications, other than those which communicate with the TOE by sending LDAP messages, shall be permitted to run on any client or server host machines which access the network, unless they have been shown not to compromise the TOE's security objectives as stated in [ST] (the equivalent restriction for the database underlying the TOE is **[OS.CA-1]** in [DBECD]).

This Page Intentionally Blank

CHAPTER

4 Configuration

This chapter describes the post-installation actions to complete the evaluated configuration.

4.1 Database Requirements

[DBECD, 4] covers the configuration requirements for the Oracle database used by OID.

4.1.1 Profile Requirement

The following requirement replaces **[DB.IA-18]** in [DBECD, 4] when configuring the database underlying the TOE.

[DB.IA-18x] After creating and setting up a database, the default profile must be changed to ProfileB, which is described in Annex A of [DBECD]. Database administrators must also employ this change to all new profiles created, to ensure that all users (including administrative users) are subject to strong password controls at all times. The guidance in [DBECD, 2.2] must be followed when modifying or creating profiles.

4.1.2 Configuring Auditing

The following provides step by step instructions detailing how to configure auditing as per **[DB.AA-2]** and **[DB.AA-7]** in [DBECD,4].

In addition, the requirements of **[DB.IA-3]**, **[DB.IA-7]** , **[DB.AA-10]** and **[DB.IA-14]** can be met by adding the parameter and its value stated in those assertions in [DBECD,4] to the parameter file during point 2 of the step by step instructions.

In this example the ORACLE_SID is `OID2`.

9. Connect to Oracle and create the pfile. This will create a file called `initOID2.ora` in the `$ORACLE_HOME/dbs` directory.

```
sql> connect / as sysdba;
sql> create pfile from spfile;
```

10. Edit the `initOID2.ora` file and add the following:

```
audit_trail = DB
```

11. Shutdown the database:

```
sql> connect / as sysdba;
sql> shutdown immediate;
```

12. Rename the spfile:

```
/dbs$ mv spfileOID2.ora spfileOID2.ora.bkp
```

13. Restart the database, run the audit script, configure auditing and create a new spfile:

```
sql> connect / as sysdba;
sql> startup;
sql> @$ORACLE_HOME/rdbms/admin/cataudit.sql
sql> audit session;
sql> show parameters; (look for audit_trail = DB)
sql> create spfile from
       pfile='/space/oracle/product/10.1.4/OIM_INFRA
       /dbs/initOID2.ora';
```

14. Auditing is now configured.

When meeting the requirements of assertion **[DB.AA-9]**, the line:
`on system.aud$`
must be replaced with:
`on sys.aud$`

4.2 TOE Requirements

The actions listed in this section are required to be performed to increase the security of the evaluated configuration after OID installation has been carried out as described in the previous chapter.

[DI.POST-1] The directory administrator must ensure that Access Control settings for the entries in the directory are such that anonymous users can only access material which the administrator deems to be “public information” (for example names of administrators and their contact telephone numbers).

An example of how Access Control settings were applied in the Evaluated Configuration by using Oracle Directory Manager is as follows:

Expand Entry Management.
Expand `cn=OracleContext`.
Select `cn=Products`.
Select the Subtree Access tab.
Under the Content Access Items section click the Create button.
Select the Attribute tab.

Scroll to and select authPassword.
Select the Access Rights tab.
Select Deny and click the OK button.
Click Apply.

One reason for establishing such Access Control settings is that the amount of information returned during a null subtree and null base search should be as restrictive as possible while still allowing operation.

[DI.POST-2] The directory administrator must establish Access Control settings for the directory so that the guest user and the proxy user can only access data that anonymous users can access. The guest and proxy users are set up with the same privileges as anonymous users during the default installation of the TOE.

[DI.POST-3] The directory administrator must set passwords of at least 8 characters in length for the guest user and the proxy user. These passwords are only to be revealed to administrators. [OIDAG, 7: Managing Super Users, Guest Users and Proxy Users] describes how to set these passwords. For example, the LDIF file to modify the guest user password would contain the lines:

```
dn:
changetype: modify
replace: orclgupassword
orclgupassword: new_password
```

The passwords for the super user and the proxy user are set by modifying the `orclsupassword` attribute and the `orclprpassword` attribute.

[DI.POST-4] The directory administrator must set a password policy for each user that can access the OID directory, which is enabled and has attributes as follows:

- `pwdMinLength` set to 6 (the minimum number of characters that may be used in a password);
- `orclpwdAlphaNumeric` set to 0 (the minimum number of numeric characters in the password);
- `pwdLockout` set to 1 (a value of 1 indicates account lockout is in force);
- `pwdMaxFailure` set to 10 (the number of consecutive failed password checks after which the user is locked out if `pwdLockout` has been set to 1); and
- `pwdLockoutDuration` set to 900 (the number of seconds for which the user is locked out when the number of consecutive failed password checks has reached `pwdMaxFailure` and `pwdLockout` has been set to 1).

[OIDAG, 19: Managing Password Policies, Accounts and Passwords] describes how to set password policies. The password policy attributes are defined in [OIDAG, 19: Password Policy Attributes]. Password policies are enabled by setting the value of the attribute `orclpwdpolicyenable` to 1.

In the Evaluated Configuration this was achieved by using an LDIF file containing the lines:

```
dn: cn=ECDPwdPolicy,cn=pwdPolicies,cn=Common,cn=Products,
cn=OracleContext
changetype: add
cn: ECDPwdPolicy
pwdMinLength: 6
```

```
orclpwdAlphaNumeric: 0
pwdLockOut: 0
pwdMaxFailure: 10
pwdLockOutDuration: 900
orclpwdPolicyEnable: 1
objectclass: top
objectclass: pwdpolicy

dn: cn=Users,dc=oracle,dc=com
changetype: modify
replace: pwdpolicysubentry
pwdpolicysubentry:  cn=ECDPwdPolicy,cn=pwdPolicies,
cn=Common,cn=Products,cn=OracleContext
```

[DI.POST-5a] The directory administrator must ensure that Access Control settings for the super user password attribute of the DSE entry (`orclsupassword`) do not allow users other than the super user to read the value of this attribute.

To do this the directory administrator must edit the default ACP to deny users access to the `orclsupassword` attribute. Using Oracle Directory Manager this can be done by navigating to the Access Control Management Panel, navigating to `Default ACP`, then creating a new ACI for attribute `orclsupassword` for which all users are denied the read, compare, search and modify capabilities.

For example:

access to attr=(orclSuPassword) by dn="cn=orcladmin"(Read, Write, Search, Compare) by * none

[DI.POST-5b] The directory administrator must ensure that Access Control settings for the hashed password attribute of the DSE entry (`authpassword`) do not allow users other than the super user to read the value of this attribute.

To do this the directory administrator must create an LDIF file to change the value of the `orclentrylevelaci` attribute to include the `authpassword` attribute. The administrator should then use the ldapmodify command line tool to apply the change.

The administrator must ensure that the current values of the `orclentrylevelaci` attribute are also included in the LDIF file.

For example, the LDIF file to modify the authpassword would contain the lines:

```
dn:
changetype: modify
replace: orclentrylevelaci
orclentrylevelaci: access to entry by * (browse, noadd, nodelete)
orclentrylevelaci: access to attr=(authpassword, orclaci, orclSuPassword) by * none
orclentrylevelaci: access to attr=(*) by * (search, read, nowrite, nocompare)
```

[DI.POST-6] The directory administrator shall ensure that the audit level is set to cover auditing of at least super user logins and user logins. The administrator should normally use an audit level that includes all security events (which is represented by a value of 16383). The directory administrator shall perform regular checks of the directory audit trail, looking for evidence of attacks against the TOE's security policy. The administrator shall ensure that the audit trail is kept to a reasonable size by archiving audit material when necessary and by purging the audit trail using `bulkdelete`.
The administrator must note that, if the directory audit trail is not regularly purged, it can cause the database to fill up. Once this has happened no actions will be audited as

there will be no space in the database to store audit records. At this point, the database administrator must make space available for the database and the directory administrator must archive audit material if necessary and then purge the directory audit trail using `bulkdelete`, as described in [OIMUR, 4: bulkdelete].

The following is a example of using the bulkdelete command to delete the auditlog:

bulkdelete connect="oid" basedn="cn=auditlog"

To ensure that the bulk command tools work correctly, environment variables must be set as specified in [OIDAG, 5: Using Command-Line Tools].

The database administrator can tell whether the database is getting full by examining the DBA_FREE_SPACE data dictionary view.

[OIDAG, 14: Setting the Audit Level] describes how to set the audit level. This can be done with an LDIF file containing the lines:

```
dn:
changetype: modify
replace: orclauditlevel
orclauditlevel: 16383
```

[DI.POST-7] The super user for the directory has the privileges necessary to perform all actions on the directory. The initial password for the super user is set by the Application Server installation process to be the same as the password for the ias_admin user for the Oracle Application Server instance. This password is supplied by the installer during the installation. The super user password should be changed after the installation process because the ias_admin password is the password for many of the Application Server tools, and hence is known by a range of Application Server administrators.
Because of the power of the super user, the directory administrator must set a password with at least 8 characters for it.

[OIDAG, 7: Managing Super Users, Guest Users and Proxy Users] describes how to set the super user password.

[DI.POST-8] The ODS schema is the database schema which holds all of the directory data. The password for the ODS database user is set by the Application Server installation process to be the same as the password for the ias_admin user for the Oracle Application Server instance. This password is supplied during the installation. The ODS database user password must be changed after the installation process because the ias_admin password is the password for many of the Application Server tools, and hence is known by a range of Application Server administrators.

[OIMUR, 3: Changing the Password to the Oracle Internet Directory Database] gives an example to show how to change the ODS password.

[DI.POST-9] The directory administrator should provide the directory server's port number to people intending to send LDAP messages to the TOE. Following installation of the TOE, the port configuration details are stored in the file `ORACLE_HOME/install/portlist.ini`. This file defines the port number that is configured to run the Oracle Internet Directory Server in non-SSL mode.

[DI.POST-10] The administrators for the system hosting the TOE shall ensure that operating system accounts and database accounts on that system are only provided for administrators.

[DI.POST-11] The `orclCryptoScheme` attribute in the DSE, which is given an initial value during the installation process, must never be set as No Encryption.

[DI.POST-12] If the administrator finds that the super user account has become locked, he or she must attempt to find the cause of the lockout before unlocking the account, and must take action to prevent re-occurrence, if possible. The administrator should also take such action if a normal user repeatedly asks the administrator to unlock their user account.

The `oidpasswd` utility in $ORACLE_HOME/bin may be used to unlock the super user account.

[OIMUR, 3: Unlocking the Super User Account] gives an example to show how to unlock the super user account.

[DI.POST-13] The administrator for Oracle database that the TOE uses to hold its directory data can use the statement:

```
AUDIT SESSION
BY ods;
```

to monitor all of the TOE's database sessions.

[DI.POST-14] In the relevant procedure in section 5.2, users must be instructed not to disclose their directory passwords to other individuals. This instruction must include the requirement that users must not change the Access Control settings for the `userpassword` attribute of their user entry to allow other non-administrative users to read the value of this attribute.

[DI.POST-15] [OIDAG, 11: Guidelines for Deleting Object Classes] states that object classes cannot be deleted from the base schema. Administrators shall therefore not attempt to delete such object classes. If items from the base schema get deleted, administrators shall employ database restore procedures to recover such items (see the relevant procedure in section 5.2 which requires that steps be taken so that the Oracle database that the TOE uses to hold its directory data can be protected against data loss).

[DI.POST-16] Password policies are described in [OIDAG, 19]. Changes to a password policy entry only take effect after the directory server instance has next been re-started. Administrators shall therefore ensure that the directory server instance is re-started when it is necessary for an updated password policy entry to take effect.

[OIMUR, 2: Restarting an Oracle Internet Directory Server Instance] given an example to show how to re-start a directory server instance.

[DI.POST-17] The directory administrator must ensure that Access Control settings for the audit log allow only administrative users to access its records.

In the Evaluated Configuration this was achieved by creating an Access Control Policy Point and an access control list via Oracle Directory Manager, as follows:

Select Access Control Management.
Click the Create button.
In the Path To Entry field enter: cn=auditlog

Under the Structural Access Items section click the Create button.
Select the By Whom tab.
Select the Specific Entry radio button and enter "cn=orcladmin" in the field.
Select the Access Rights tab.
Click the OK button.

Again under the Structural Access Items section click the Create button.
Select the By Whom tab.
Select the Everyone radio button.
Select the Access Rights tab.
Select all the Deny radio buttons and click the OK button.

On the Select Access Control Management pane click the OK button.

[DI.POST-18] The directory administrator must ensure that the Referential Integrity feature is enabled as described in [OIDAG, 12]. Once this has been done, then, whenever a user's entry in the directory is deleted or its DN is updated, OID also updates the groups that this user was a member of when the `$ORACLE_HOME/ldap/admin/oidrimdx.pls` script is next run.

The directory administrator must cause this script to be run as frequently as is necessary for the site-specific needs, but every 15 minutes to 24 hours is a normal range. If a directory entry has been deleted or its DN has been modified and the administrator has to get the other directory entries updated immediately to accommodate this change in the interests of maintaining the security of the directory, then the administrator must explicitly run the `oidrimdx.pls` script as soon as possible. Otherwise the administrator should consider running the script via a `cron` job.

If the directory administrator needs to know whether the Referential Integrity feature is enabled, he or she should check whether there are entries:
cn=ri_postdelete,cn=plugin,cn=subconfigsubentry and
cn=ri_postmoddn,cn=plugin,cn=subconfigsubentry
in the directory, because such entries are created when the feature is enabled and are deleted to disable the feature. To find out whether there are outstanding updates to be performed to maintain referential integrity, the directory administrator should check whether there are any rows in the Referential Integrity storage table `t_rimoddel` in OID's Oracle database. Each such entry indicates an update to be performed next time the `oidrimdx.pls` script is run.

[DI.POST-19] The directory administrator must ensure that Access Control settings for each password policy entry allow only administrative users to modify it. Thus all users will be able to access the password policy, but attempts to make modifications will give rise to an error message stating Insufficient Access Rights. All attempts at changing the password policy are auditable.

In the Evaluated Configuration this was achieved by creating an Access Control Policy Point and an access control list via Oracle Directory Manager to prevent anonymous access to the password policies, as follows:

Select Access Control Management.
Click the Create button.
In the Path To Entry field enter:
`cn=pwdPolicies,cn=Common,cn=Products,cn=OracleContext`

Under the Structural Access Items section click the Create button.
Select the By Whom tab.
In the Authentication Choice: select Simple.
Select the Access Rights tab.

Click the OK button.

Again under the Structural Access Items section click the Create button.
Select the By Whom tab.
In the Authentication Choice: leave this blank.
Select the Access Rights tab.
Select all the Deny radio buttons and click the OK button.

On the Select Access Control Management pane click the OK button.

[DI.POST-20] There may be interactions if an administrator is using a TOE directory administration tool described in [OIDAG, 5: Using Command-Line Tools] to access data which is simultaneously being accessed by a directory server instance executing an LDAP request. Guidance on action to be taken to avoid any such undesirable interactions is given in the documentation for each TOE directory administration tool in [OIMUR, 3] and [OIMUR, 4]. If administrators are in doubt about possible interactions, they must ensure that the directory server is not running when they use a TOE directory administration tool.

[DI.POST-21] The administrator must ensure that the operating system's auditing is started by using the following command:

```
$ /etc/init.d/auditd start
```

In addition the administrator must ensure auditing is automatically started on reboot as follows:

```
$/sbin/chkconfig auditd on
```

[DI.POST-22] The directory administrator must ensure the Group Cache and Entry Cache are disabled. In the Evaluated Configuration this was achieved by using Oracle Directory Manager to set the values of Enable Entry Cache and Enable Group Cache to zero.

[DI.POST-23] The directory administrator must ensure that ACIs are not applied directly to user accounts. Instead, each ACI must be applied at the Group level and users added to the appropriate Group. Administrators should create Groups in the directory to represent users' roles. If possible, such groups should not be deleted, although, at a particular point in time, there may be no members of that group.

If there is a requirement to modify the DN of or delete any Groups, the directory administrator must check whether there are any ACIs that reference the Group and, if so, amend the ACIs accordingly.

CHAPTER

5 Procedures

The procedural requirements for maintaining the security of the database system underlying the TOE are given in [DBECD, 2.2]. This chapter describes additional procedural requirements for maintaining the security of the TOE.

5.1 Operating System Procedures

5.1.1 General Procedures

[OS-2] The operating system administrator shall ensure that only designated users are able to perform administrative tasks within the operating system. In addition, the only local operating system user accounts on the server shall be those for the TOE software administrator (e.g. the oracle user account) and the operating system administrator account (e.g. the root account).

[OS-3] The operating system administrator shall ensure that there are no general purpose computing capabilities (e.g. compilers or user applications) available on the TOE servers other than those services necessary for the operation, support and administration of the TOE software.

5.1.2 Identification and Authentication

[IA-1] Non-administrative users (existing or newly created) shall not belong to the administrative groups in either the host machine on which the TOE is installed, or on a local client machine from which they will connect to the TOE. See [OS-2] for guidance about such administrative groups.

[IA-2] All normal operating system users shall have a non-administrative primary group set, such as USERS.

5.1.3 Protection of Resources

[PR-1] The operating system shall protect all of the installed TOE-related files and directories by means of its Access Control Mechanisms to ensure that they are accessible to their authorised users only. The Oracle Universal Installer sets file permissions when the Oracle software is installed, so no further action in this respect is required.

[PR-2] To maintain the integrity of the audit timestamp, only registered system administrators

shall have access to the operating system clock configuration. All other users shall have no access permissions for the operating system clock configuration.

[PR-3] Authorised administrators of the TOE are non-hostile, are appropriately trained and follow administrator best practice and guidance.

5.1.4 Accounting and Auditing

[AA-1] The operating system shall protect operating system audit trails or any other audit trails (e.g. audit log files) used by the TOE against unauthorised modification and deletion by means of its Discretionary Access Control mechanisms.

[AA-2] The directory containing the TOE-generated audit log files shall have permissions set for only the local TOE administrator operating group and no access for all other users.

[AA-3] The operating system administrator shall adopt procedures to archive audit log files prior to audit trail size or disk space exhaustion.

5.2 TOE Administration Procedures

Procedures for the administration of TOE security shall be established based on the contents of this document, the Security Target [ST], any site security policy that may be in force and [DBECD]. In particular, procedures for the TOE shall be established as follows:

- The directory administrator shall instruct users not to disclose their directory passwords to other individuals.
- The directory administrator shall advise users of the restrictions on the passwords they can use as a result of the settings in the directory password policies that apply to them.
- Directory user passwords generated by the system administrator shall be distributed in a secure manner.
- Procedures and/or mechanisms shall assure that, after system failure or other discontinuity, recovery without a protection (i.e. security) compromise is obtained. Such procedures shall include steps to be taken so that the Oracle database that the TOE uses to hold its directory data can be protected against data loss. The subject of database backup and recovery is covered in [OBRC].
- The on-line and off-line storage media on which security related data (such as audit trails) is held shall be properly stored and maintained, and routinely checked to ensure the integrity and availability of the security related data;
- The media on which directory-related files (including database files, export files, redo log files, control files, trace files, and dump files) have been stored shall be purged prior to being re-used.
- The directory super user is a highly trusted user, who is required by the architecture of the TOE to be able to perform privileged directory administration operations such as setting of the audit level and setting access control permissions for users. It is necessary that appropriate personnel and procedural measures (such as procedural two-person control) will be provided to ensure that operations performed under this trusted user account conform to the system security policy.
- For more routine administration tasks it is recommended that alternative, less privileged, directory user accounts are used. These accounts should be configured

as members of administrative groups and should be used to perform a set of resticted administrative operations for the directory.

Note that, on the completion of installation, OID provides 2 similarly named administrative accounts that have different levels of privilege:

a) the directory super user with the DN of "cn=orcladmin" and

b) an administrative account with the DN of "cn=orcladmin, cn=Users, dc=oracle,dc=com"

To perform a given administrative action, the account should be used that has the minimum level of privilege neccessary for the action.

- Administrators, through the use of password policies, shall ensure that password controls for all users (including trusted administrative users) are strong enough to satisfy the TOE's CC Strength of Function rating of SOF-*high*.
- Administrators should be aware of the factors influencing the strength of user passwords when creating or updating password policies. **[DI.POST-4]** ensures that certain limits are set in every password policy. However, suitable use of the other available password controls normally strengthens the TOE's overall password mechanism strength.
  For example, setting `pwdMaxAge` (Password Expiry Time) in conjunction with `pwdExpireWarning` (Password Expiration Warning) will limit the opportunity of an attacker to guess a particular password. In addition, using `pwdInHistory` (Number of Password History) will ensure passwords held in the history store cannot be re-used, again limiting the opportunity for a particular password to be guessed. To prevent the same password being supplied again at the end of a password lifetime period, administrators should set `orclpwdToggle` (Old Password Can Be New Password) to 0.
  Note that Password policies are described in [OIDAG, 19]. The password policy attributes are defined in [OIDAG, 19: Password Policy Attributes].

This Page Intentionally Blank

ANNEX

A TOE Components

A.1 Server components

The components that are installed on the server by the Oracle Universal Installer during the installation of Oracle Internet Directory 10*g* (10.1.4.0.1) are listed in the install log. This can be located in the following directory:

`/space/oracle/oraInventory/logs`

A.2 Evaluated Configuration Boundaries

The evaluated configuration of the TOE shall comprise exactly the following software components:

- Oracle Internet Directory 10.1.4.0.1
- Oracle Internet Directory Server 10.1.4.0.1
- Oracle Internet Directory Tools 10.1.4.0.1

A.3 Client components

There are no client components in the TOE.

This Page Intentionally Blank

B Red Hat Installation

This Annex describes the steps required to install RedHat Enterprise Linux 4 Update 5 on a server in the Evaluated Configuration for Oracle Internet Directory 10*g* (10.1.4.0.1) or in the Evaluated Configuration for Oracle Identity and Access Management 10*g* (10.1.4.0.1). [ECGR4] may be read for general guidance when installing Red Hat.

The information that was supplied by the administrator for each step during the installation of the Red Hat software for the evaluation of the TOE is indicated in the section below.

B.1 Installation Steps

Insert the RedHat Linux Enterprise Edition Update 4 boot CD into the server CD Drive.

Start up the server - if the server is currently running, reboot it. Note that the following steps will overwrite all data.

Press F11 to enter the Boot Device Menu.

Use the arrow keys and select IDE CD-ROM device.

At the boot prompt, enter linux askmethod.

Linux will start to boot.

Choose a language for the installation - English was selected.

Choose a Keyboard type - UK was selected.

Choose the installation method based on the location of the installation media and click OK. NFS was selected.

Select a network device and click OK. eth0 was selected.

Enter the networking configuration - a static IP address is required for the evaluated configuration.

Enter NFS Server Name and directory name for the location of the installation media. SAGfs1t.saglab.uk.oracle.com and /vol/KITS/Software/RedHat/RHEL4U5 was entered.

The installation will proceed and a graphical installer will load.

Click next at the Welcome screen.

Select Install RedHat Enterprise Linux AS and click Next.

Select Manually Partition with Disk Druid and click Next.

If partitions already exist, click Remove all partitions on this system and click Next.

To create a Partion, click New and then enter the partion details: Mount Point, File System Type, Size and Additional Size Options. The following partitions must be created:

Mount Point	Type	Size (Mb)	Options
/	Ext3	10000	Fixed Size
/space	Ext3	50000	Fixed Size
/tmp	Ext3	10000	Fixed Size
/home	Ext3	10000	Fixed Size
<na>	Swap	20000	Fixed Size

Table 5-1:

When all partitions are created, click Next.

Click Next to use the GRUB boot loader (default setting).

The Networking information should already be present if the installation has been performed using NFS. Otherwise, specify the Networking information at this point - the Evaluated Configuration must have static IP addresses for both servers. When complete, click Next.

No Firewall was configured for the Evaluated Configuration on the Firewall Configuration screen. (A firewall will be manually configured after all of applications have been installed).

Click Next to continue from the Firewall Configuration screen.

On the Addition Language Support screen, English (USA) was de-selected and English (Great Britain) was selected. Click Next.

Time Zone Europe/London was selected and Next clicked.

Next, enter a password for the root user. This password must consist of Alphabetic characters and at least one Numeric character.

On the Package Installation Defaults screen, select Customise Software Packages option and click Next.

The following must be selected:

X Window System - keep the defaults.

GNOME desktop Environment - remove all optional packages except gnome-libs.

Editors - select the Group.

Graphical Internet - uncheck all optional Packages with the exception of Firefox.

Text based Internet - deselect the Group.

Web Server - deselect the Group.

Windows File Server - deselect the Group.

Development Tools - remove all except the kernel packages.

Legacy Software Development - select the Group.

Printing Support - deselect the Group.

Click Next. The Installer will format the disk andinstall the packages.

The installer will prompt for a reboot. Once this has taken place a Welcome screen is presented. Click Next.

Agree to the licence and click Next.

If there is a NTP server on the network, enter its details on the Date and Time Network Time Protocol tab. Otherwise, enter time details manually. Click Next.

Configure a display as appropriate. Click Next

On the RedHat Login page, select the 'Tell me why…' option and click next.

Click the 'I can not complete…. ' option and click Next.

Enter a System User. This must be a general Administration user, such as admin. Provide an appropriate password and click next.

Click Next on the Additional CDs screen.

Click Next on the Finish Setup Screen.

The server will now start and show a login prompt.

This Page Intentionally Blank

ANNEX

C References

[CC] *Common Criteria for Information Technology Security Evaluation,* Version 2.3, August 2005.

[DBECD] *Evaluated Configuration for Oracle Database 10g Release 1 (10.1.0),* Issue 0.5, November 2005, Oracle Corporation.

[ECD904] *Evaluated Configuration for Oracle Internet Directory 10g (9.0.4),* Issue 0.4, November 2004, Oracle Corporation.

[ECGR4] *CC EAL4+ Evaluated Configuration Guide for Oracle Enterprise Linux 4 U4 and U5, Version 1.3*, 23rd August 2007, Oracle Corporation.

[LDAP3] *Lightweight Directory Access Protocol (v3),* Request For Comments (RFC) 2251 of the Internet Engineering Task Force, December 1997, available on the World Wide Web at http://www.ietf.org/rfc.htm

[OBRC] *Oracle Database Backup and Recovery Basics 10g Release 1 (10.1),* Part No. B10735-01, Oracle Corporation.

[OIDAG] *Oracle Internet Directory Administrator's Guide 10g (10.1.4.0.1),* Part No. B15991-01, Oracle Corporation.

[OIDIG] *Evaluated Configuration for Oracle Identity and Access Management 10g (10.1.4.0.1): Oracle Internet Directory Installation,* Oracle Corporation**.**

[OIMUR] *Oracle Identity Management User Reference 10g (10.1.4.0.1),* Part No. B15998-01, Oracle Corporation.

[INST] *Oracle Application Server Installation Guide 10g (10.1.4.0.1) for Linux x86,* Part No. B28194-01, Oracle Corporation.

[ST] *Security Target for Oracle Internet Directory 10g (10.1.4.0.1),* Oracle Corporation**.**